Using FortiManager as a FortiGuard Distribution Server for Fortinet Products in Closed Network Environments

Contents

Fortinet VMs available in closed networks

The following devices can be deployed in a closed network by uploading a service entitlement file to a FortiManager and allowing the device to validate it's VM licence with the FortiManager:

- FortiADC
- FortiGate
- FortiMail
- FortiWeb

The following devices can be deployed in a closed network without requiring to validate their VM licence with FortiGuard. Instead the VM licence is tied to the IP address of the VM:

- FortiAnalyzer
- FortiAuthenticator
- FortiManager
- FortiRecorder
- FortiSandbox
- FortiVoice

The following devices be deployed in a closed network without requiring to validate their VM licence with FortiGuard. Instead the VM licence is tied to the VM:

- FortiNAC – Uses the UUID and the MAC address of eth0 interface
- FortiSIEM – Uses the VM UUID

Internet Connectivity only for FortiManager

How to configure FortiManager

Web UI

- System Settings -> Network -> Interface -> portX
  - Enable Service Access for FortiGate Updates and Web Filtering

CLI

```
config system interface
    edit "port1"
        set ip <IP address> <netmask>
        set allowaccess ping https ssh http
        set serviceaccess fgtupdates webfilter-antispam
        config ipv6
        end
    next
end
```

Debugging

Checking registered licenses

```
diagnose fmupdate vm-license
```

Sample Output

```
fmg $ diagnose fmupdate vm-license

VM License Cache Size: 3
Cache Entry Key=FGVM1VTM19001327
    Serial: FGVM1VTM19001327
    UID   : 20038f2a5b16e751454633ebaaa67232
    status: 200
    Active   Time: UTC 1576030598  Local 2019/12/11 03:16:38
    Register Time: UTC 1573163597  Local 2019/11/07 22:53:17

Cache Entry Key=FVVM020000187074
    Serial: FVVM020000187074
    UID   : 8e51f6fc8c9151e9578a679c5ae5dff1
    status: 200
    Active   Time: UTC 1576082578  Local 2019/12/11 17:42:58
    Register Time: UTC 1576082578  Local 2019/12/11 17:42:58

Cache Entry Key=FVVM020000189598
    Serial: FVVM020000189598
    UID   : aa422518060642cf9718453e304be86f
    status: 200
    Active   Time: UTC 1576077317  Local 2019/12/11 16:15:17
    Register Time: UTC 1576077317  Local 2019/12/11 16:15:17
```

Get debug information about FortiManager requests to FortiGuard

```
fmg $ diagnose debug application fgdsvr 255
```

Get debug information about products requesting updates

```
fmg $ diagnose debug application fdssvrd 255
```

Re-fining log settings

For debugging purposes, you can change what logs appear in the FortiManager event logs:

```
config fmupdate fds-setting
fmtr-log                fmtr log level
linkd-log               The linkd log level (default = info).
```

Possible values:

```
alert         Log level - alert
critical      Log level - critical
debug         Log level - debug
disable       Disable linkd log
emergency     Log level - emergency
error         Log level - error
info          Log level - info
notice        Log level - notice
warn          Log level - warn
```

FortiManager as a FortiGuard Distribution Server behind a Proxy

If FortiManager can access FortiGuard servers through an HTTP proxy, it will by default contact FortiGuard servers via HTTP. It can be configured on CLI to use HTTPS.

HTTPS:

```
config fmupdate av-ips web-proxy
    set ip <proxy-ip-addr>
    set mode tunnel
    set port <proxy-port>
    set status enable
end

config fmupdate web-spam web-proxy
    set ip <proxy-ip-addr>
    set mode tunnel
    set port <proxy-port>
    set status enable
end

config fmupdate fds-setting
    set fds-clt-ssl-protocol tlsv1.2
    set fds-ssl-protocol tlsv1.2
end
```

Fortinet VM licensing using Entitlement Files

This section focuses on the Fortinet VMs that operate in closed mode via the use of service entitlement files uploaded to a FortiManager.

Registering Fortinet VM with Customer Service & Support

To obtain the Fortinet VM licence file you must first register your Fortinet VM with Customer Service & Support.

To register your Fortinet VM:

1. Log in to the Customer Service & Support portal using an existing support account or select **Sign Up** to create a new account.

2. In the main page, under **Asset**, select **Register/Renew**.

   The **Registration** page opens.

3. Enter the registration code that was emailed to you and select **Register**. A registration form will display.

4. After completing the form, a registration acknowledgement page will appear.

5. Select the **License File Download** link.

6. You will be prompted to save the licence file (`.lic`) to your local computer. Refer to "Upload the licence file" for instructions on uploading the licence file to your Fortinet VM via the Web-based Manager.

Enabling FortiManager to validate VM licences

FortiManager can be used to validate the VM licences and the subscribed services of FortiADCs, FortiGates, FortiMails, and FortiWebs in closed networks. In order to do so, after having purchased VM licences and registered them on https://support.fortinet.com, you must request a service entitlement file from Fortinet's support team, and then upload the service entitlement file to the FortiManager.

Requesting entitlement files for VM licences

To request the service entitlement file from Fortinet support:

1. On the Fortinet Technical Support web site (https://support.fortinet.com/) create a ticket with Fortinet Technical Support by going to **Assistance** > **Create Ticket** > **Customer Service** > **Submit Ticket**.

2. Enter the serial number. Under **Category**, select **CS Contact/License**.

3. In the Comment field, ask for an "entitlement file" for your Fortinet VMs. Provide the serial number and licence number. If you don't remember them, you can find them in **Asset** > **Manage View Products** > `<Select product>`.

Example:
Serial Number: FGVM010000024628
License Number: FGVM0035444

Note: Alternatively, as with registration, you can attach a spreadsheet that contains serial and licence numbers if you want to ask for entitlement files for two or more Fortinet VMs at the same time. Fortinet Technical Support will provide one entitlement file that contains validation information for all of your Fortinet VMs. All Fortinet VMs must be registered with the same account; devices registered under different accounts cannot be combined into the same entitlement file.

Uploading the entitlement file to FortiManager

FortiManager can be used to validate the VM service entitlements of FortiADCs, FortiGates, FortiMails, and FortiWebs:

1. Log into the FortiManager GUI and click **FortiGuard** > **Advanced Settings**.
2. If not already checked, check **Disable Communication with FortiGuard Servers** and click **Apply**.
3. Go to **FortiGuard** > **Advanced Settings** > **Upload Options for FortiGate/FortiMail** > **Service License** and upload the entitlement file.
4. To verify the configuration, once you've configured other Fortinet VMs with an override to use FortiManager as their local FDN server, you can reboot them or use their CLI commands to force them to send a new VM licence validation request to FortiManager. If validation succeeds, the licence status indicated on the dashboard should say **Valid**.

FortiManager as a FortiGuard Distribution Server in a closed network

FortiManager can be used as a FortiGuard Distribution Server for providing AntiVirus and IPS updates, and web filtering and spam filtering. To enable this on the FortiManager:

1. Log into the FortiManager GUI and click **FortiGuard** > **Settings**.
2. Click **Enable Communication with FortiGuard Servers** to show as **ON,** and then click **Apply**.
3. Check **Enable AntiVirus and IPS Update Service** to **ON** and enable the checkboxes for all devices and firmware versions under management, then optionally click **Apply.**
4. Optionally, if there is an upstream FortiManager being used to FortiGuard Distribution Server, click on the **FortiGuard AntiVirus and IPS Settings >** label to expand the options, and then enable **Use Override Server Address for**

FortiGate / FortiMail. In the newly expanded section click the **+** sign that has appeared on the right to add a new entry. Fill in the IP address of the upstream FortiManager, and click **Apply**.

5. Optionally, if there is an upstream FortiManager being used to FortiGuard Distribution Server, click on the **FortiGuard Web Filter and Email Filter Settings >** label to expand the options, and then enable **Use Override Server Address for FortiGate / FortiMail**. In the newly expanded section click the **+** sign that has appeared on the right to add a new entry. Fill in the IP address of the upstream FortiManager, and click **Apply**.

6. Wait until FortiManager has downloaded and synchronized all the service packages and updates. This could take several hours. The status for the downloading of the Web Filter and Email Filter databases can be seen under under **FortiGuard** > **Settings**. Check also the status of the downloads under:

   FortiGuard > **Query Server Management** > **Receive Status** for the Web Filter and Email Filter download status
   and
   FortiGuard > **Package Management** > **Receive Status** for the AntiVirus and IPS download status

7. If the status under **Receive Status** appears stuck, i.e. the date and timestamp remains untouched across any package after waiting for a few hours. You can manually trigger to update the packages:
   ```
   diagnose fmupdate fds-updatenow
   diagnose fmupdate fgd-updatenow
   ```

8. After the packages and updates are synchronized, click **FortiGuard** > **Settings** and click **Enable Communication with FortiGuard Servers** to **OFF**. Click **Apply**.

Configure Fortinet VMs to use FortiManager

FortiManager

If the FortiManager is not already configured to be in closed mode, the following CLI commands configure it to no longer communicate with the FortiGuard Distribution Network (FDN):

```
config fmupdate publicnetwork
set status disable
end
```

FortiADC

These commands will disable the FortiADC's direct communication with FortiGuard and force the FortiGate to use the FortiManager in order to validate it's VM licence:

```
config system fortiguard
set override-server-status enable
set override-server-address <IPv4 address of FortiManager
device>:8890
end
```

There is no command to force a FortiADC to immediately validate it's VM licence with the FortiManager. The quickest way to verify that the FortiADC can validate it's VM licence with the FortiManager is to reboot the FortiADC which can be done with the command:

```
execute reboot
```

Note: Without using entitlement files, FortiADC cannot validate the license through FortiManager. Also, it cannot receive updates from FortiManager, because FortiManager (up to version 6.2.4) does not support FortiADC.

FortiGate

These commands will disable the FortiGate's direct communication with FortiGuard and force the FortiGate to use the FortiManager in order to validate it's VM licence:

```
config system central-management
set mode normal
set type fortimanager
set fmg <IPv4 address of the FortiManager device>
set fmg-source-ip <IPv4 address on FortiGate used when connecting to
the FortiManager device>
set include-default-servers disable
set vdom <Enter the name of the VDOM to use when communicating with
the FortiManager device>
end
```

These commands will enable the FortiGate to use the FortiManager as a FortiGuard Distribution Server for retrieving AV updates, IPS packages, web filtering, and spam

filtering:

```
config system central-management
config server-list
edit 0
set type update rating
set server-address <IPv4 address of the FortiManager device>
end
end
```

The following command will force the FortiGate to immediately check in with the configured FortiGuard servers, which if configured correctly should now be the FortiManager, to validate it's VM licence, and service entitlement:

```
execute update-now
```

FortiMail

These commands will disable the FortiMail's direct communication with FortiGuard and force the FortiMail to use the FortiManager in order to validate it's VM licence and to use the FortiManager as a FortiGuard Distribution Server for retrieving AV updates, and spam filtering:

```
config system fortiguard antivirus
set override-server-status enable
set override-server-address <IPv4 address of FortiManager
device>:8890
end
```

The following command will force the FortiMail to immediately check in with the configured FortiGuard servers, which if configured correctly should now be the FortiManager, to validate it's VM licence, and service entitlement:

```
execute update-now
```

FortiWeb

These commands will disable the FortiGate's direct communication with FortiGuard and force the FortiGate to use the FortiManager in order to validate it's VM licence:

```
config system autoupdate override
set status enable
set address <IPv4 address of FortiManager device>:8890
set fail-over disable
end
```

The following command will force the FortiWeb to immediately check in with the configured FortiGuard servers, which if configured correctly should now be the FortiManager, to validate it's VM licence, and service entitlement:

```
execute update-now
```

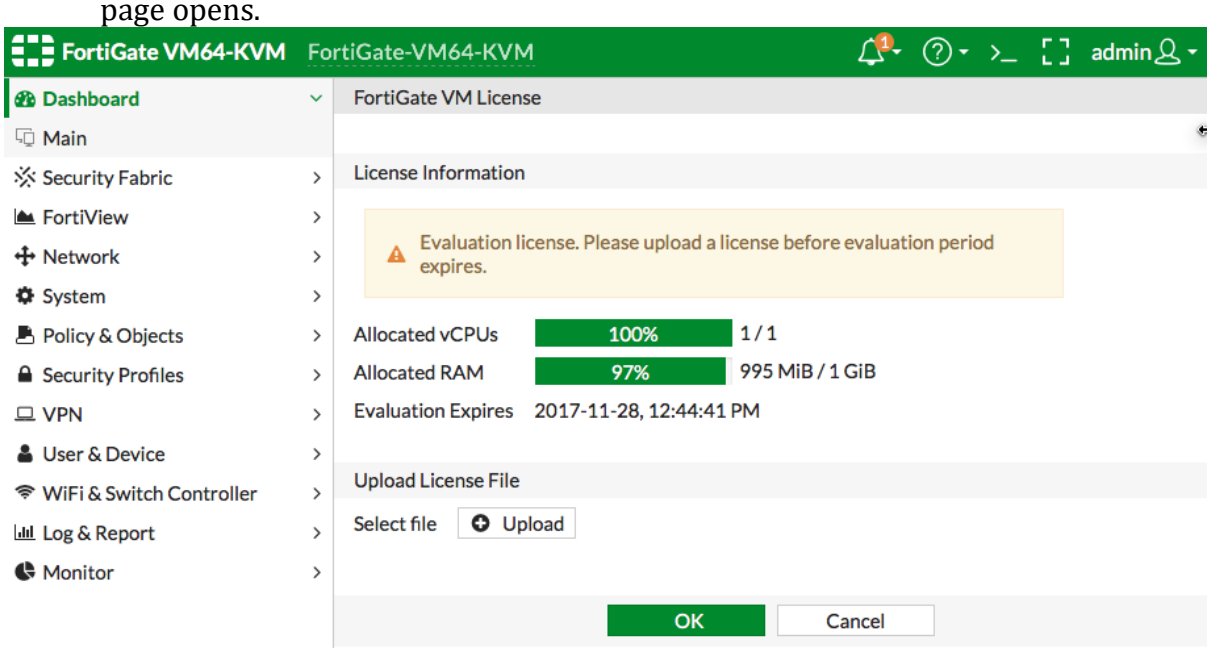
Debugging

```
diag debug enable
diag debug application fds 7
execute update-now
diag system update info
```

Upload the Fortinet VM licence file

To upload the Fortinet VM licence file:

1. In the Fortinet VM License dialog box, select **Enter Licence**. The licence upload page opens.



2. Select **Upload** and locate the licence file (`.lic`) on your computer. Select **OK** to upload the licence file.
3. Refresh the browser to login.
4. Enter `admin` in the Name field, or your username and password, and select Login. The VM registration status appears as valid in the **License Information** widget once the licence has been validated by the FortiGuard Distribution Network (FDN) or FortiManager for closed networks.

Note: Modern browsers can have an issue with allowing connections to a FortiGate if the encryption on the device is too low. Adjusting browser settings does not normally mitigate the issue. If this happens, Admins must use a FTP/TFTP server to apply the licence.

CLI

You can also upload the licence file via the CLI using the following CLI command:

```
execute restore vmlicense [ftp | tftp] <filenmame string> <ftp server>[:ftp port]
```

Example:

The following is an example output when using a TFTP server to install the licence.

```
exec restore vmlicense tftp license.lic 10.0.1.2
This operation will overwrite the current VM license! Do you want to continue? (y/n) y
Please wait...Connect to tftp server 10.0.1.2 ...
Get VM license from tftp server OK.
VM license install succeeded.
Rebooting firewall.
```

Fortinet VMs using IP address

This section focuses on the Fortinet VMs that operate in closed mode via the use of a VM licence that verifies its licence via a management IP address.

Register Fortinet VM with Customer Service & Support

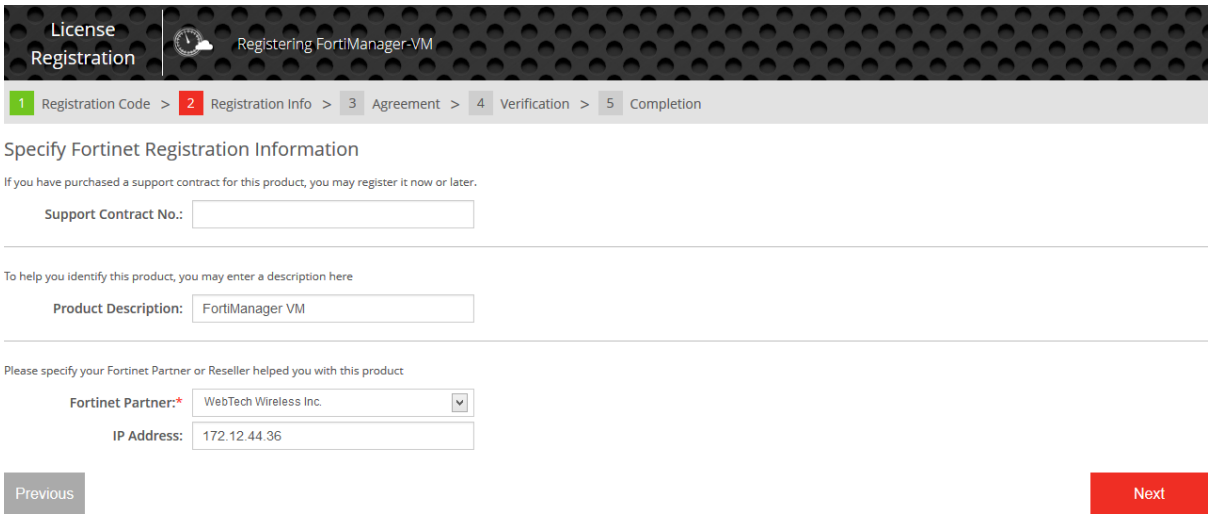
To obtain the Fortinet VM licence file you must first register your Fortinet VM with Fortinet Customer Service & Support.

To register your Fortinet VM:

1. Log in to the Fortinet Customer Service & Support portal using an existing support account or click **Create an Account** to create a new account.

2. In the toolbar select **Asset** > **Register/Renew**. The **Registration Wizard** opens.

3. Enter the registration code from the Fortinet VM License Certificate that was emailed to you, select the end user type, and then click **Next**. The **Registration Info** page is displayed.



4. Enter your support contract number, product description, Fortinet Partner, and IP address in the requisite fields, then select **Next**.

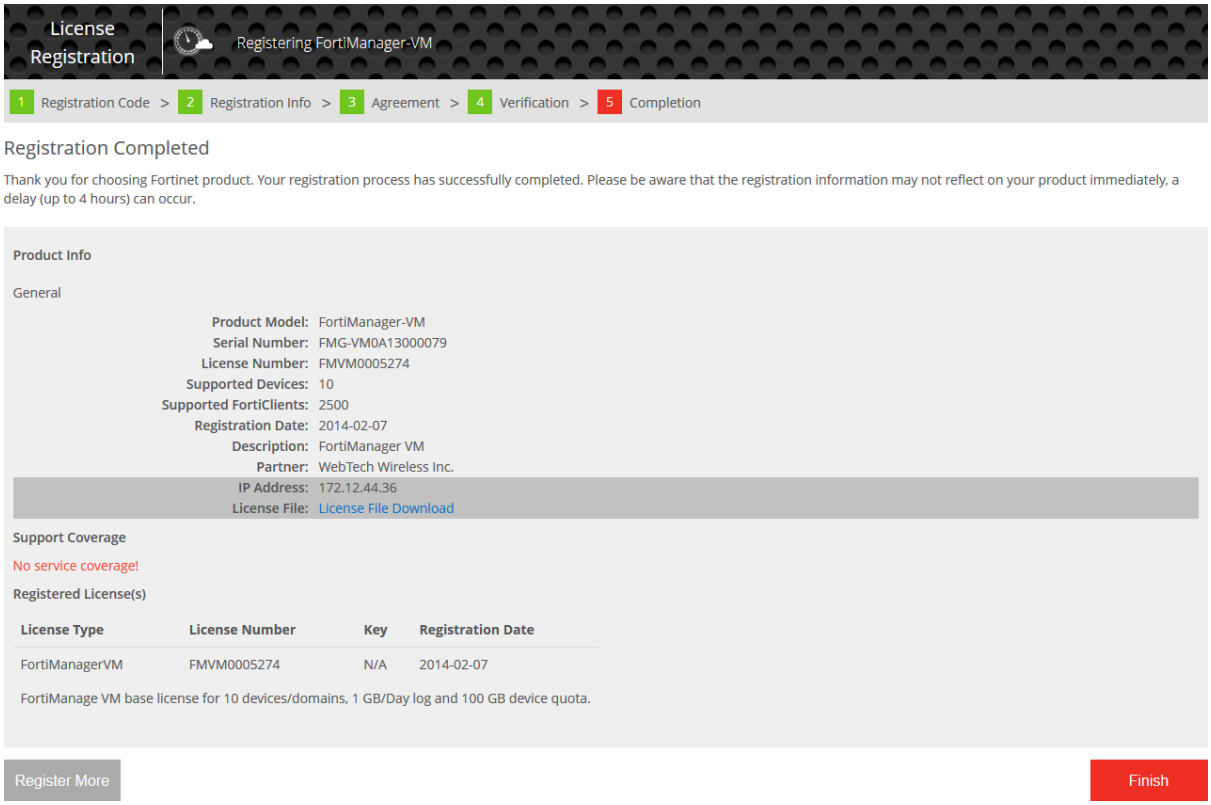
   Note: As a part of the licence validation process Fortinet VM compares its IP address with the IP information in the licence file. If a new licence has been imported or the Fortinet VM's IP address has been changed, the Fortinet VM must be rebooted in order for the system to validate the change and operate with a valid licence.

   Note: The Customer Service & Support portal currently does not support IPv6 for Fortinet VM licence validation. You must specify an IPv4 address in both the support portal and the port management interface.

5. On the **Fortinet Product Registration Agreement** page, select the checkbox to indicate that you have read, understood, and accepted the service contract, then

select **Next** to continue to the **Verification** page.

6. The verification page displays the product entitlement. Select the checkbox to indicate that you accept the terms then select **Confirm** to submit the request.



7. From the Registration Completed page you can download the Fortinet VM licence file, select **Register More** to register another Fortinet VM, or select **Finish** to complete the registration process.

   Select **License File Download** to save the licence file (.lic) to your management computer. See Upload the licence file for instructions on uploading the licence file to your Fortinet VM via the GUI.

Upload the licence file

Before using the Fortinet VM you must enter the licence file that you downloaded from the Customer Service & Support portal upon registration.

To upload the licence via the CLI:

1. Open the licence file in a text editor and copy the VM licence string.
2. In a Fortinet VM console window, enter the following:
   ```
   execute add-vm-license <"vm license string">
   ```
   Refer to the CLI Reference for the particular Fortinet VM, available from the Fortinet Document Library, for more details on using this command.

To upload the licence file via the GUI:

1. In the **Evaluation License** dialog box, select **Enter License**.

Optionally, if you are replacing an existing VM licence on the Fortinet VM you can also select **Upload License** in the **License Information** dashboard widget.

2. In the licence upload page, click **Browse**, locate the VM licence file (`.lic`) on your computer, then click **OK** to upload the licence file.

   A reboot message will be shown, then the Fortinet VM system will reboot and load the licence file.

3. Refresh your browser and log back into the Fortinet VM with username `admin` and no password, or your username and password if already configured.

   The VM registration status appears as valid in the **License Information** widget once the licence has been validated.

Note: As a part of the licence validation process Fortinet VM compares its IP address with the IP information in the licence file. If a new licence has been imported or the Fortinet's licenced IP address has been changed, the Fortinet VM must be rebooted in order for the system to validate the change and operate with a valid licence.

If the IP address in the licence file and the IP address configured in the Fortinet VM do not match, an error message will be displayed after logging back into the VM.

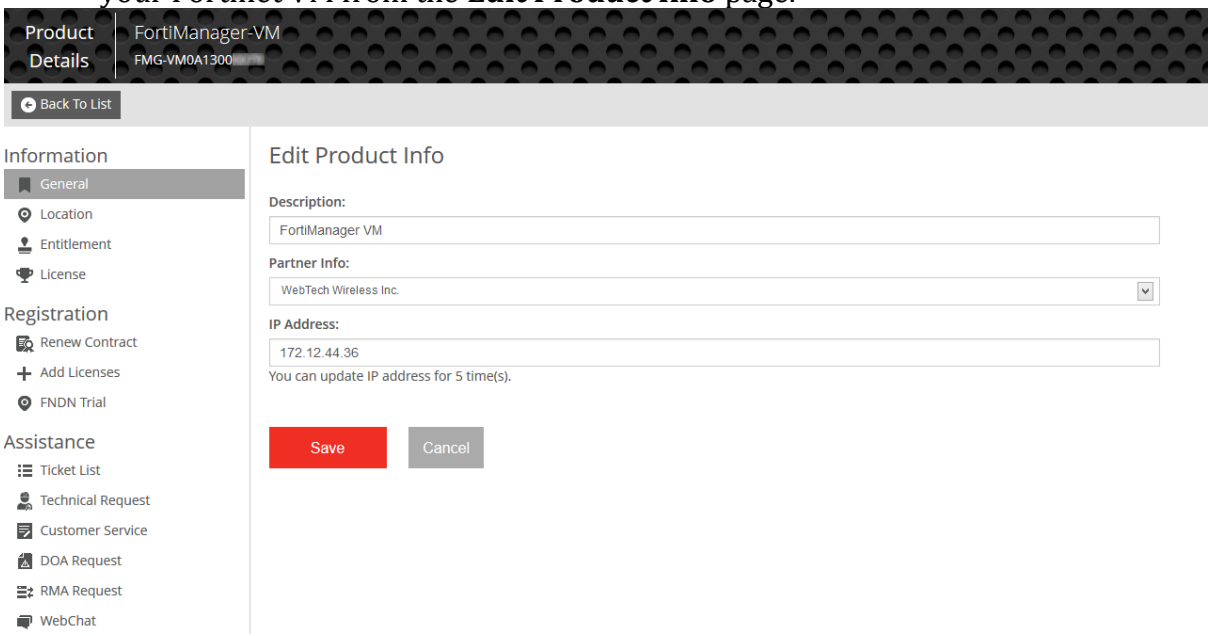
If this occurs, the IP address will need to be changed in the Customer Service & Support portal to match the management IP and re-download the licence file. To change the management IP address, refer to Editing the Fortinet VM IP address below.

Note: After an invalid licence file has been loaded onto the Fortinet VM, the GUI will be locked until a valid licence file is uploaded. A new licence file can be uploaded via the CLI.

Editing the Fortinet VM IP address

In the event that the Fortinet VM's IP address needs to change, then follow the below steps.

1. In the toolbar select **Asset** > **Manage/View Products** to open the **View Products** page.
2. Select the Fortinet VM serial number to open the **Product Details** page.
3. Select **Edit** to change the description, partner information, and IP address of your Fortinet VM from the **Edit Product Info** page.



4. Enter the new IP address then select **Save**.

   Note: You can change the IP address five (5) times on a regular Fortinet VM licence. There is no restriction on a full evaluation licence.

5. Select **License File Download** to save the licence file (.lic) to your management computer.

Fortinet VMs using UUIDs

This section focuses on the Fortinet VMs that operate in closed mode via the use of a VM licence that verifies its licence via a management IP address.

FortiNAC

Set the IP Address for eth0

Note: When a FortiNAC Control Server and Application Server are paired, configure the FortiNAC Application Server virtual machine first to assign an IP address. The FortiNAC Control Server must know the IP address of the FortiNAC Application Server in order to communicate with it.

To configure FortiNAC you must access the Configuration Wizard using the IP address of eth0. Eth0 is the management interface for FortiNAC. Follow the instructions below to set the IP address for eth0.

1. Make sure the FortiNAC virtual machine is running and the console is displayed.

2. Login to the FortiNAC CLI using the following:
   User name = `admin`
   Password = `admin`

3. You must select an IP address to use as the management IP for the FortiNAC VM. To set the IP address, type the following:
   `sudo configIP <IP address> <netmask> <default gateway>`
   Example:
   `sudo configIP 192.168.5.244 255.255.255.0 192.168.5.1`

4. The system pauses for several seconds while the interfaces are reset.

5. To confirm that the IP address for eth0 has been set correctly, type the following:
   ip addr show

6. Repeat this process for each FortiNAC VM.

Licence Key

Each FortiNAC virtual machine requires its own unique licence key. Upon purchasing FortiNAC, an Authorization Code is provided. This is a one-time use code and allows the customer to self-generate the licence key themselves during installation.

Note: Licence Keys that need to be regenerated due to licence count increase, appliance transitions, etc., are provided by Fortinet through its original Bradford Networks URL.

To generate a licence key, you must know the Authorization Code, the MAC address of eth0 and the UUID of each VM.

Note: When a FortiNAC Control Server and Application Server are paired, configure the FortiNAC Application Server virtual machine first to assign an IP address. The FortiNAC

Control Server must know the IP address of the FortiNAC Application Server in order to communicate with it.

1. Access the Configuration Wizard by opening a browser on your PC and navigating to:
   `http://<IP address>:8080/configWizard`
   IP address is the address of eth0 that you configured earlier in the process. Refer to Set the IP Address for eth0.

2. Enter the Configuration Wizard credentials.
   User Name = `config`
   Password = `config`

3. The **License Key Validation** window is displayed.

4. Make sure you have the Authorization Code given to you when you purchased FortiNAC. Make note of the UUID and eth0 MAC lines on the License Key screen. You can copy and paste these into the licence key generator.

5. To access the licence key generator, open a separate browser window and navigate to: https://license001.bradfordnetworks.com/authcode-keygen/

6. Enter the Authorization Code, UUID and eth0 MAC in the appropriate fields in the licence key generator and click **Generate License Key**.

   Note: You should have received an email with your Authorization Code from Fortinet when you purchased FortiNAC. If you do not have this code, contact your Sales Representative.

7. Copy the licence key that is created to the **License Key** field in **the Configuration Wizard**.

8. Click **OK** at the bottom of the License Key Validation window.

FortiSIEM

As FortiSIEM does not maintain a connection to FortiGuard in order to validate its VM licence there is no difference between deploying FortiSIEM in a closed network or an open network.

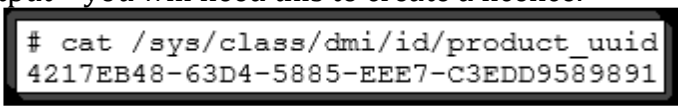
To licence a FortiSIEM VM, the FortiSIEM Supervisor node must first be deployed. This guide focuses solely on VM licensing and does not cover the deployment of the FortiSIEM Supervisor node. For this, please refer to the FortiSIEM Licensing Guide for more information on the end to end deployment and licensing of FortiSIEM.

In order to licence a FortiSIEM VM, the hardware ID of the FortiSIEM must first be obtained, as this is used in order to register the FortiSIEM and create the licence file.

Hardware ID

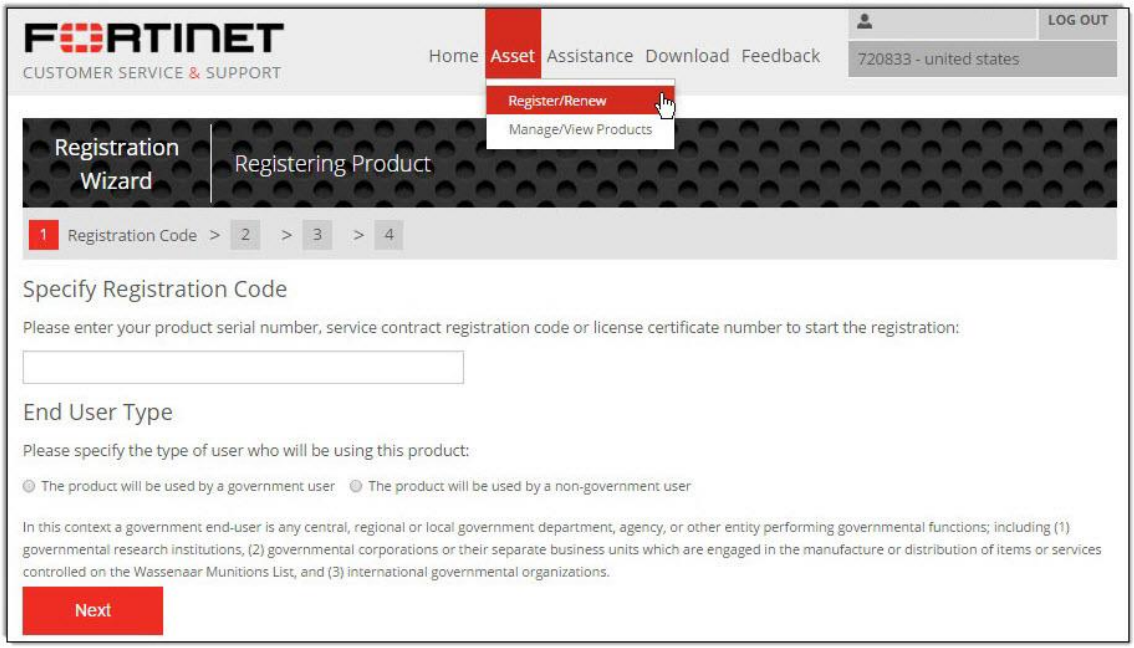
The Hardware ID (UUID) is used to uniquely identify the server where FortiSIEM Supervisor node will run.
Follow one of the methods below:
Open **https://<ip_of_supervisor>/**.
The licence upload page displays the Hardware ID.
Go to the server where FortiSIEM Supervisor node has to be installed or is currently installed.

1. Login via SSH as `root`.
2. Run the command `cat /sys/class/dmi/id/product_uuid`
3. Note the output – you will need this to create a licence.

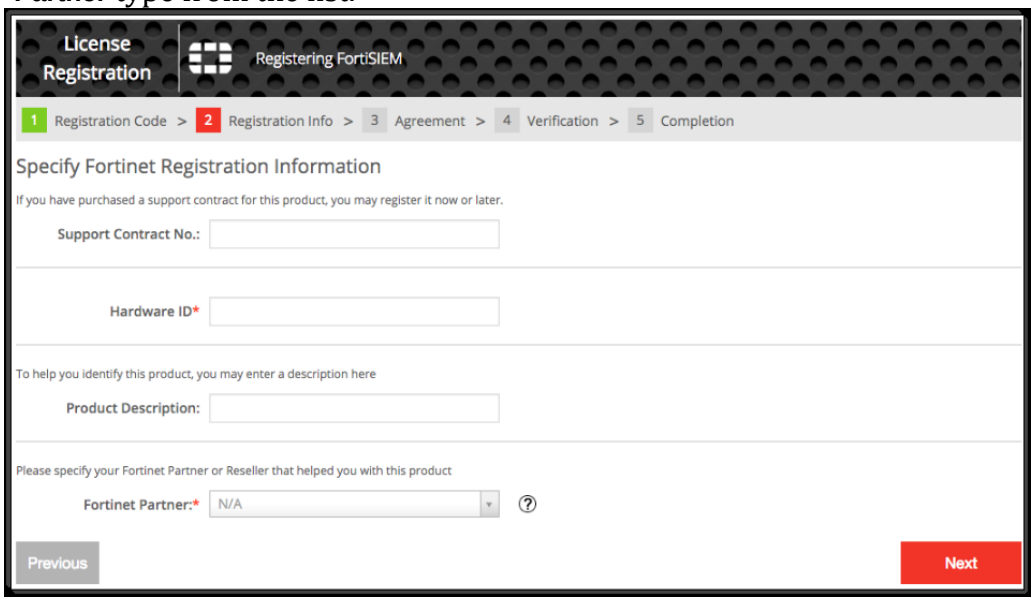


Register the FortiSIEM VM and deploy the VM licence

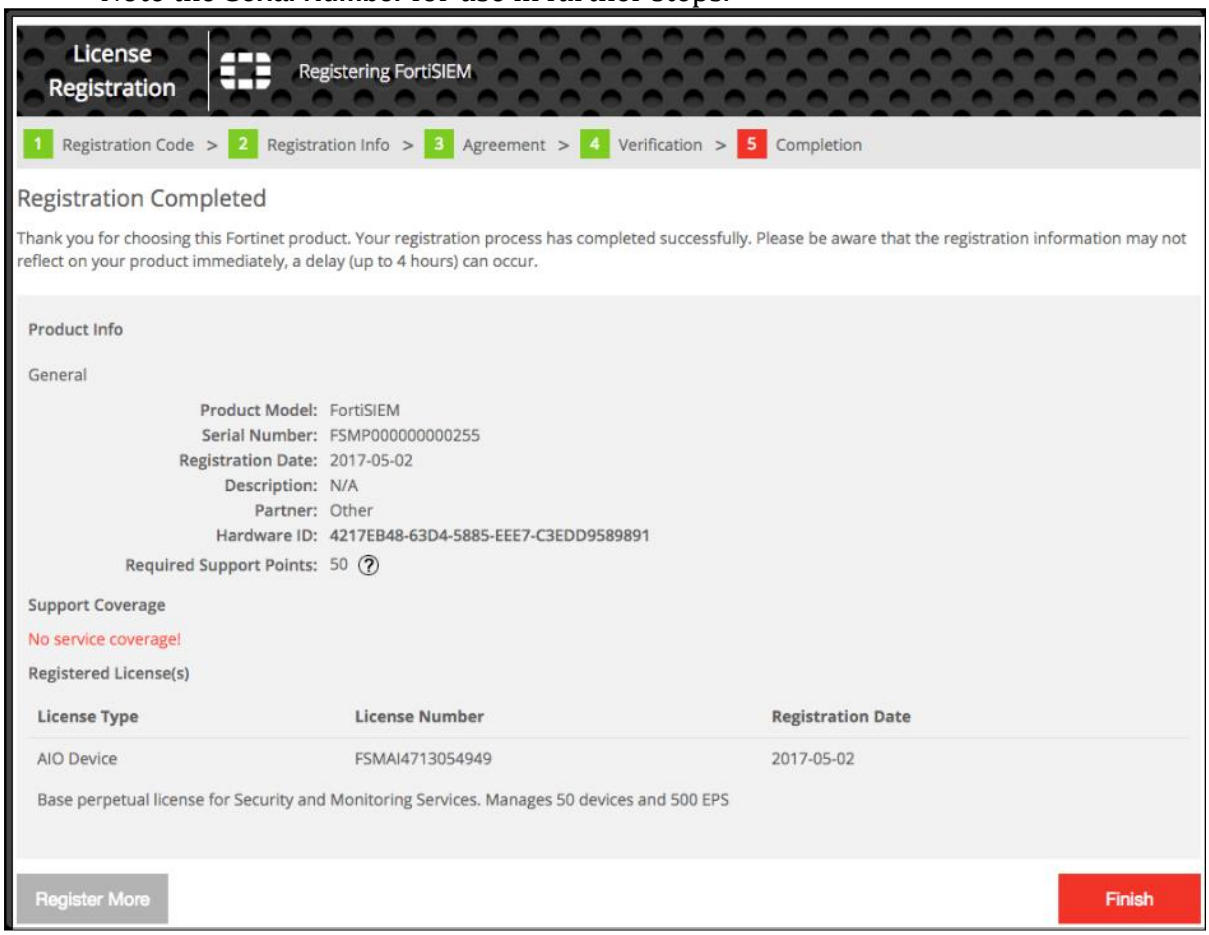
1. Go to FortiCare Product Registration link: https://support.fortinet.com/
2. Click **SIGN UP** to create an account.
3. Log in using your **Account ID/Email** and **Password**.
4. Click **Asset** > **Register/Renew** and enter the **Registration Code** of the Base licence based on the licence type.
    - **Subscription based licence**: Open the SKU file corresponding to the Subscription based licence:
      FC*[1-8]-10-FSM98-180-02-DD* and get the Registration code.
    - **Perpetual licence**: Open the SKU file corresponding to the Base Perpetual Licence:
      FSM-AIO-BASE and get the Registration code.



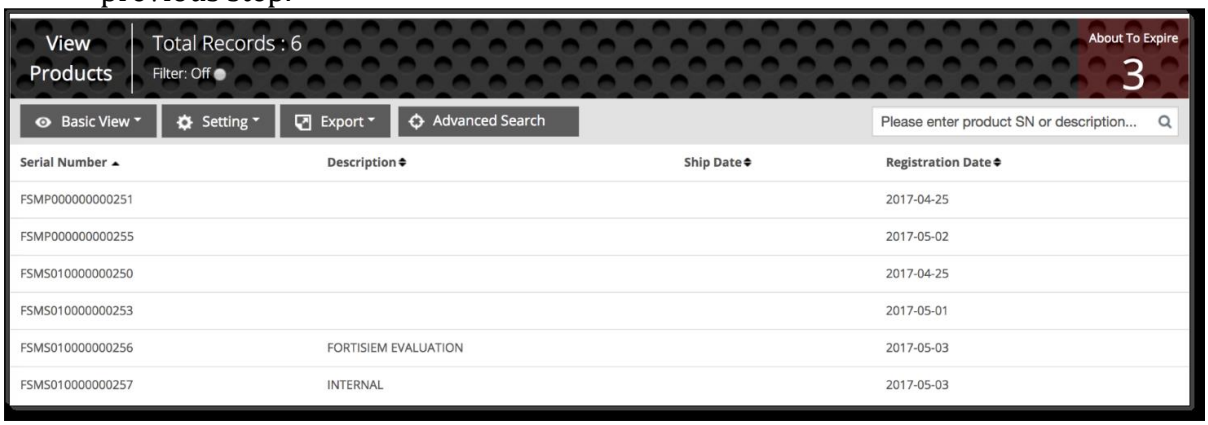
5. Select the **End User Type** and click **Next.**
6. On the **License Registration** page, enter the **Hardware ID** and select the **Fortinet Partner** type from the list.



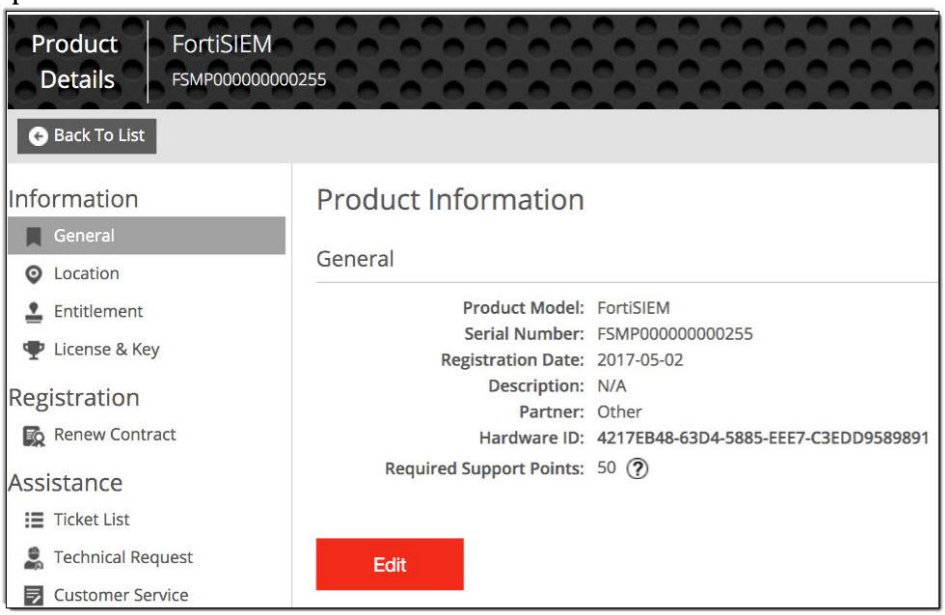
7. Click **Next.**
8. Read and agree to the terms and conditions of **Fortinet Product Registration Agreement** and click **Next**.
9. On the **Verification** page, read and agree to the terms and click **Confirm.**
10. Verify the information displayed under **Product Info** and click **Finish.**
    Note the **Serial Number** for use in further steps.



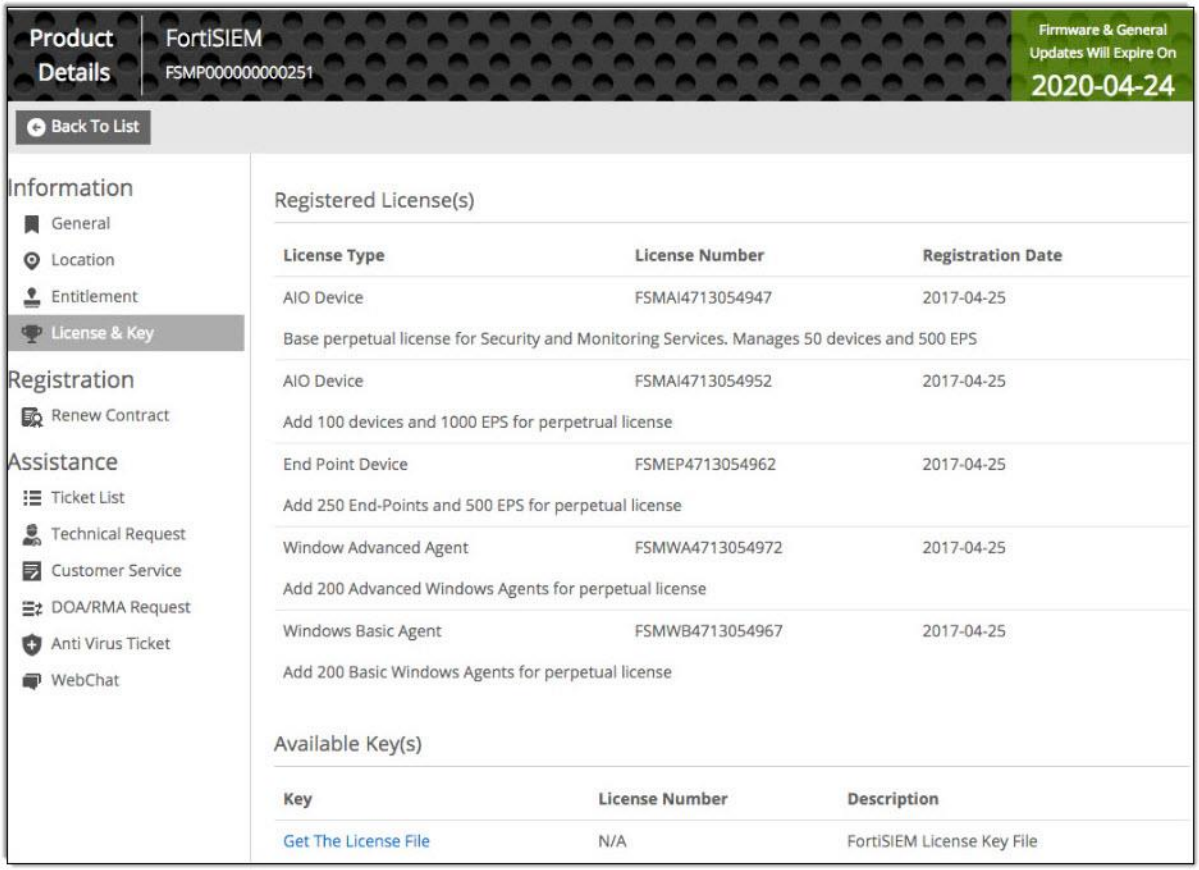
11. Go to **Asset** > **Manage/View products** and click the **Serial number** obtained from the previous step.



12. Select **General** and click **Edit** to associate the Hardware ID of the VM where the Supervisor is going to run. The Hardware ID can be obtained by following the steps in Hardware ID.



13. Select **License & Key** and click **Get The License File** link to download the licence.



14. Once FortiSIEM is installed, log in and click **Browse** to select the licence file.
    Note: If the UI does not redirect to the licence upload screen, open https://<ip_of_supervisor>/phoenix/licenseUpload.html and upload the licence file.

15. Enter the **User ID** (default value: *admin)* and **Password** (default value: *admin*1*).
16. Select the **License Type** based on the deployment type as:
    - **Enterprise** for single organizations
    - **Service Provider** for multiple organizations

    Note: For earlier versions of FortiSIEM, the License Type options displayed were VA for Enterprise and **SP** for Service Provider.
17. Click **Upload** which is enabled after selecting the licence file.